CS 235: Algebraic Algorithms, Spring 2021

Discussion 1

Date: Tuesday, February 02, 2021.

Problem 1. For all integers $a, b, c > 0$. Show that:

(a) $\gcd(ca, cb) = c\ \gcd(a, b)$ and $\text{lcm}(ca, cb) = c\ \text{lcm}(a, b)$

(b) $d = \gcd(a, b) \neq 0$ if and only if $\gcd(a/d, b/d) = 1$

Hint: recall from the lecture, if $d = \gcd(a, b)$ then we can express d as a linear combination of a, b, namely, $ax + by = d$ for some $x, y \in \mathbb{Z}$

part a: lcm(ca, cb) = c lcm(a, b), let d = lcm(ca, cb) and e = c lcm(a, b)
to show: d =< e (1), e =< d implies d = e (2)

(1) On the one hand, lcm(a, b) = ax = by for some integers x, y
c lcm(a, b) = cax = cby = e --> e is a common multiple of both ca and cb
since d = lcm(ca, cb), therefore, d =< e

(2) On the other hand, lcm(ca, cb) = cax = cby = d for some integers x, y
d = cax = cby => d/c = ax = by which implies that d/c is a common multiple of both a & b
lcm(a, b) =< d/c => c lcm(a, b) =< d => e =< d

Hence, e = d ./.

first part: d = gcd(ca, cb) and e = c gcd(a, b), strategy: d >= e; e>=d --> d = e

part b: "=>" given: d = gcd(a, b), to show gcd(a/d, b/d) = 1

express d as: ax + by = d for some integers x, y
--> a/d x + b/d y = 1 --> gcd(a/d, b/d) = 1

"<=" given gcd(a/d, b/d) = 1, to show d = gcd(a, b)
gcd(a/d, b/d) =1 --> a/d x + b/d y = 1
---> ax + by = d
suppose, for the sake of contradiction, we a common multiple c > d
(ax)/c + (by)/c = d/c (contradiction because d/c is not an integer)

Problem 2. Let $a, b, n \in \mathbb{Z}$ with $n > 0$ and $a \equiv b \pmod{n}$ Show that $\gcd(a, n) = \gcd(b, n)$.

Problem 3. Let $a \in \mathbb{Z}$, show that: $a^2 \not\equiv 2 \pmod 4$ or $a^2 \not\equiv 3 \pmod 4$

Hint: consider we have $a \equiv n \pmod 4$, then what are the possible values for n? Then, for each n, how can we express a in terms of some $x \in \mathbb{Z}$? At this point, what is special about a^2 in terms of x?